MALWARE INTELLIGENT INTRUSION, DEDUCTION AND PROTECTION USING MACHINE LEARNING TECHNIQUES

SYNOPSIS

Submitted by

SATHIYANDRAKUMAR SRINIVASAN
(Reg. No. 201906242)

in partial fulfilment for award of the degree of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER APPLICATION
SCHOOL OF COMPUTING
KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
ANAND NAGAR, KRISHNANKOIL – 626126
TAMILNADU, INDIA

MAY 2023

1. INTRODUCTION

Cyber security is a process that's designed to protect networks and devices from external threats. The businesses typically employ cyber security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services [1]. The world of cyber security revolves around the industry standard of confidentiality, integrity, and availability (CIA). Privacy means data can be accessed only by authorized parties; Integrity means information can be added, altered, or removed only by authorized users; Availability means systems, functions, and data must be available on-demand according to agreed-upon parameters [2]

The main element of cyber security is the use of authentication mechanisms. For example, a username identifies an account that a user wants to access, while a password is a mechanism that proves the user is who he claims to be.

The cyber security is classified into various categories as below but not limited to

- Asset security: Analyse networks, computers, routers, and wireless access points
- Security architecture and engineering: Standardize security policies and procedures
- Communication and network security: Regulate cloud storage and data transfer
- Identity and access management: Track user authentication and accountability
- Security operations: Monitor security to identify attacks
- Security assessment and testing: Test security policies to ensure compliance with industry standards

The benefits of security are tremendous including below mentioned.

- Protect enterprises infrastructure and individual/customer information
- To find, test, and repair weaknesses within a company's infrastructure
- Monitor systems for malicious content
- Identify network breaches; Install regular software updates, firewalls, and antivirus protection

- Strengthen areas where attacks may have occurred
- Securing passwords
- Installing regular updates

2. LITERATURE SURVEY

In the modern era, digital devices are a part of everyday life. Easy access to the internet across the globe has totally changed the pattern of life; the web has become the main source of acquiring knowledge and information as stated by Mohd Anul Haq et al.[3]. Email is replacing the postal mail system. Use of computers is mandatory from the primary education sector to government level enterprise. Social media is becoming the main way to communicate socially. All these developments have made the life of people easier and comfortable but at the same time crimes associated with technology are also emerging. Cyber security related to information compromise has become a vital issue. The common people are unaware of standard practices for cyber security as stated by Bhuvansehwari et al. [4]. The government and corporate are still vibrant regarding cybercrime related issues. Dong. et al. [5] performed an in-depth survey about the awareness of cyber security issues across the globe. This survey has been conducted using various methods which include both online and offline versions of the survey. The study finds that there is a patchy awareness level, and it is not satisfactory.

2.1 Survey on Ensemble Behavioural model

Ensembles are predictive models that combine predictions from two or more other models. Ensemble learning methods are popular and the go-to technique when the best performance on a predictive modelling project is the most important outcome. Nevertheless, they are not always the most appropriate technique to use and in the field of applied machine learning have the expectation that ensembles or a specific ensemble method are always the best method to use as suggested by Bagui et al. [6].

Ensembles offer two specific benefits on a predictive modelling project. It is important to know what these benefits are and how to measure them to ensure that using an ensemble is the right decision on the research. When using this model, Peters et al. [7] conveyed that though the model increases the data flow, it lacks in classifications.

2.2 Survey on Interactive Behaviour Analysis model

The expanse of software and IT in the past couple decades has fundamentally transformed the world we live in and how we interact with the world. Engineers have learned how to store data on how users interact with software down to how the user moves their mouse. By itself this collected data would not be extremely helpful. However, improved analytics capabilities in recent years, especially in artificial intelligence, have enabled massive amounts of user data to be mined for insights as intimated by Ali et a. [8]. Analysing large amounts of user data in this manner is called as behavioural analytics. Abdellah and Koucheryavy [9] have developed a Named Entity Recognition (NER) System which helps to classify the malware and its characteristics. However, Barthakur et al.[10] reported that this model is not applicable to all the malware types as this model deduction is vary with respect to type of malwares.

2.3 Survey on Memory Forensics model

Memory forensics (Sometimes referred to as memory analysis) refers to the analysis of volatile data in a server memory dump. Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviours that do not leave easily detectable tracks on hard drive data. Fayaz et al. [11] presented a unique generative method based on the convolution seq2seq framework. In comparison to the classic RNN seq2seq paradigm, a hierarchical CNN design is extremely effective. A copying technique is used for managing unseen/rare terms in these models. Siracusano et al. [12] also incorporated a concurrent hierarchical attention approach for modelling essential sentences.

2.4 Survey on Data Stage model

The DataStage model is an industry-leading data integration tool that helps us to design, develop and run jobs that move and transform data. At its core, the DataStage tool supports extract, transform and load (ETL) and extract, load and transform (ELT) patterns. From the existing literature survey, it was found that there is a need for highly precise information extraction and case outcome prediction techniques, better scheme for document summarization and classification of malware

deductions. Hence, this research focuses on providing methodologies to overcome these existing challenges in cyber security.

3. RESEARCH PROBLEM

According to the conducted research, the following are the common and persisting issues in the legal arena.

- The research related to analysis of malware is one of the main challenging areas due to evolving various malware
- The existing research is focusing on auto detection works based on how the database has been configured and how the record set has been configured. On other hand, the hash value will match only the specific database approach and will not validate any other parameter [13]. This is a challenge to detect the malware for non-database related aspects. This has the limitation as it detects only specific types of malwares
- The large and extra-large bytes of information have been transferred in between the network bumps in every nano second, which gives space for unauthorized person's access to going to the systems and networks. This will be challenging to detect, identify and rectify
- Increasing the false positive and this leads to significant analysis of false cyber attack
- The various data approaches from various sources and in various formats is a significant challenge. The research is trying to use various tools to identify and rectify the issues. However, it's quite challenging so far [14]. The research needs to come up with various ideas along with artificial intelligence help for this solution.

4. RESEARCH OBJECTIVE

Our major research focus is to develop an effective cyber security and deduction outcome prediction method and to use mitigation measures to reduce the threat and deductions. This leads us to have the following as our research objectives.

- **Objective 1:** To identify real users and anomalous user level access from robots with unusual variation in the number of servers accessed over time using a regression base model.
- **Objective 2:** To identify users who have a high positive or negative slope to find users with unusual activity
- **Objective 3:** To identify high-value use cases to solve security risks using security analytics

5. PROPOSED METHODOLOGY

The proposed research begins with a deep learning based multi perspective analysis. The systematic study has been conducted aimed at the field of malware analytics as a main contender. It has analysed various data sets which are created by malware unlimitedly while evolving. This provides protracted history and helps to understand and learn accordingly. Also, we analysed what frequency the malware spreads and what is the impact it has. Based on that analysis, we understand the malwares threat and ways to alleviate the threats. As a part of the in-depth analysis, we found that multi perspective analytics is required to investigate further on malware analysis and remediate them.

The machine learning perspective of machine learning is a technique which helps to understand the patterns in the predictive method. Machine Learning helps where we deduct the malwares in predictable fashions. The malware deduction is simplified using machine learning because of its predictive patterns. The prediction method helps for simplified analysis and managed operations. This is also helping simplified implementation of malware deductions. The perspective of this approach using machine learning is analysing the malwares which involves two basic components.

1. Feature generation - Gathering malware and its patterns are from the regular samples,

2. Machine learning perspective – Applying various reverse engineering factors and strategies for various analysis to debug the programs such as custom programs for further analysis.

This machine learning perspective helps to identify anomalous user-level behaviour models using lateral movement deduction. Figure 1 describes the proposed method.

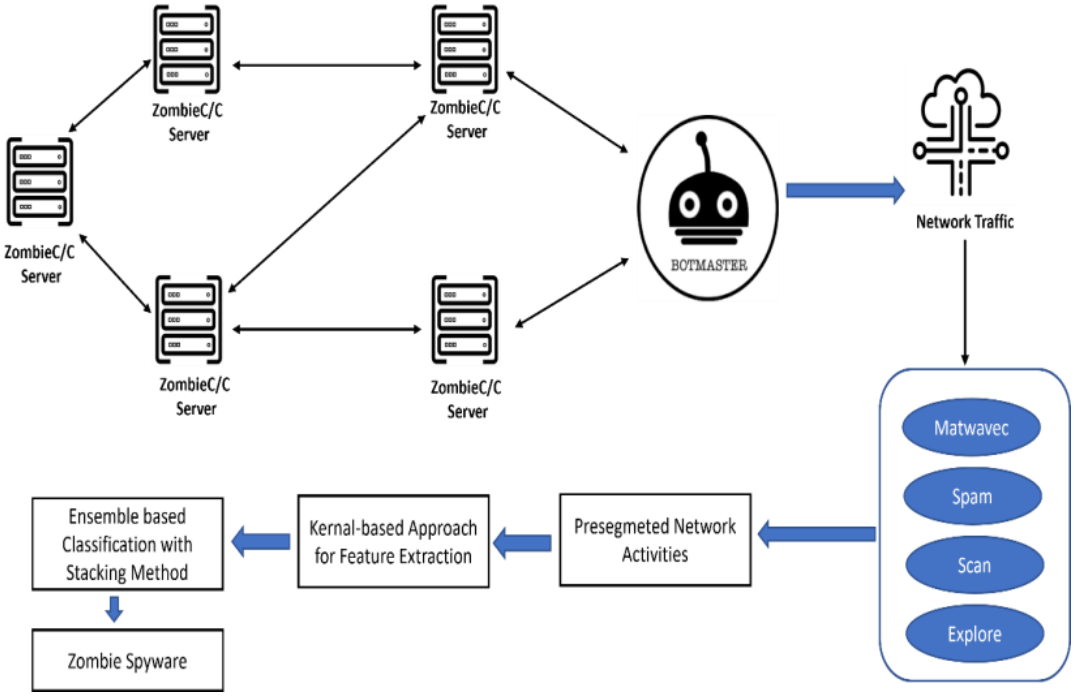

Figure 1: Architecture of the proposed botnet classification method

5.1 Deep learning based Opinion Mining

The proposed model emphases the Command and Control (C&C) channel, that is assumed as the bots are in a preliminary communication phase and applying this model at this stage is advantageous. The proposed classification method in which pre-processing is the initial stage where redundancy is eliminated, and data normalization is performed. During selection of features, the most valuable features are obtained, which are provided as input to ML methods to determine the model's performance. The better one is chosen followed by this process for the detection of botnets at the C&C's initial stage. The proposed botmaster connected with the internet and connected through the C&C servers which directly interacted through the workstation. The architecture of botmaster is shown in Figure 2.

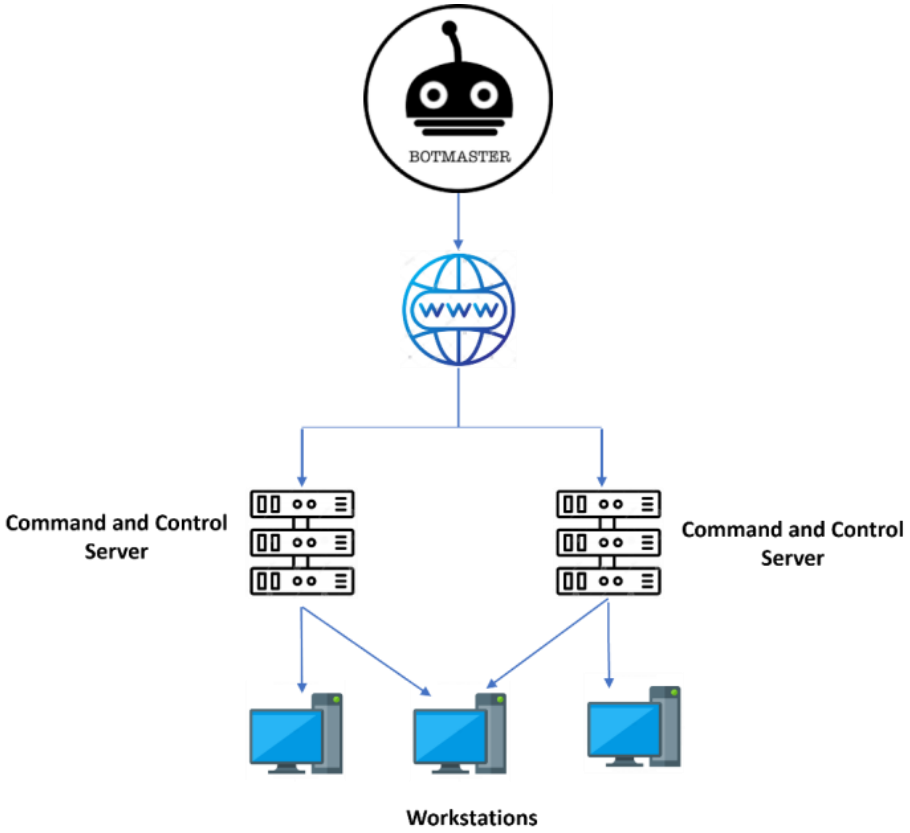

Figure 2: Proposed botmaster interaction model

5.1.1 Feature selection using kernel method

The data processing is applied to produce a clean corpus. The kernel trick's ultimate benefit is that the objective function we're optimizing to match the higher-dimensional decision boundary only incorporates the modified feature vectors' dot product. As a result, we can simply use the kernel function to replace these dot product expressions. The feature selection process is optimized with this scheme.

For the training data D, a set of points n is given by as indicated the below equation:

$$D = \{(x_i, y_i)_{i=1}^{n}, x_i \in R^d and \ y_i \in \{+1, -1\}\} \qquad (1)$$

The non-zero α_j^* are termed as support vectors which generate optimal hyperplane for separation as indicated in below equation:

$$w^{*T}\phi(x) + b^* = \sum_{j=1}^{n} \alpha_j^* y_j k(x_i, x_j) + b^* = 0 \qquad (2)$$

Two steps decompose the problem: finding out best weights, β_l by using the sparse solution, and reducing soft margin error function by involving linear programming.

5.1.2 Ensemble classification with stacking process

The ensemble learning is the act of intentionally generating and combining many models, such as classifiers or experts, to solve a computer intelligence issue. Ensemble learning is mostly used to boost performance (classification, prediction, function approximation, etc.). In general, an ensemble F contains a set of predictors of a function fi' as indicated as the below equation

$$F = \{ fi' , i = 1, ..., k\} \quad (3)$$

The learner model can train data-producing outcomes used for final predictions. Multiple sub-learners can be selected as stacking specifies alternate models to learn the best combination of forecasts. The meta-model shown in Figure 3 combines these predictions from the sub-models, this approach is even known as blending since final predictions are combined.

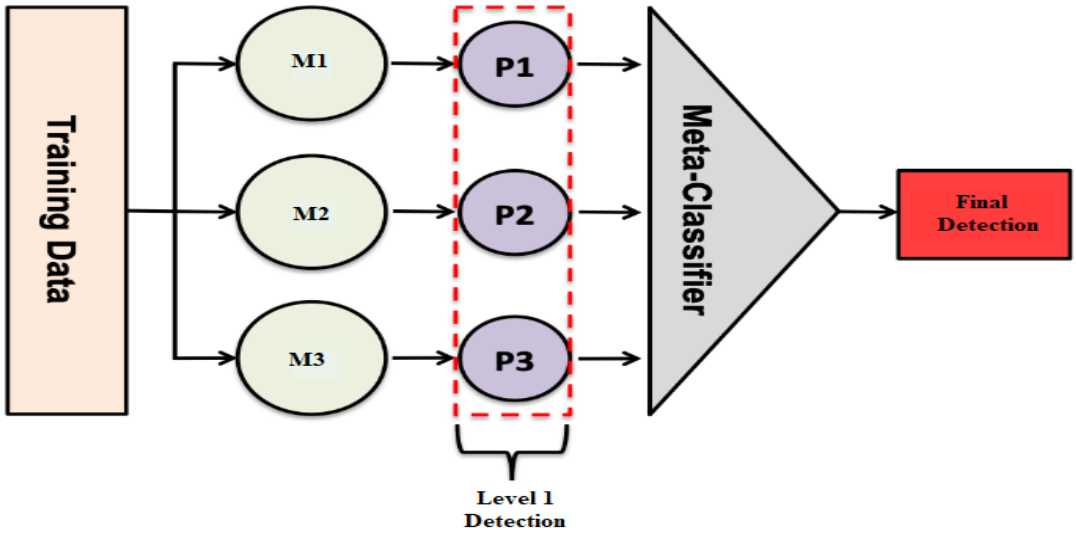

Figure 3: Ensemble classification process

.5.1.3 Experimental analysis

Accuracy (Acc): The proportion of total correctly classified bugging and debugging datasets to the total number of bugging and debugging reports as stated in equation.

Sensitivity (Sc) is the ratio of the negative instances that are classified incorrectly and is determined as stated in equation.

Specificity (Sp) is the ratio of the positive instances that are correctly classified and is determined as stated in equation.

F-Measure is the combination of precision and recall producing a single measure stated in equation.

Table 1 describes the comparison of the accuracy between the existing methods and proposed method.

Table 1: Comparison of accuracy

No. of data packets	ELM	CNN	SVM	ECASP [proposed]
50	88.2	89.2	90.3	91.2
100	89.5	90.5	91.6	93.5
150	92.5	92.5	93.5	94.5
200	93.8	94.8	95.1	95.2
250	94	95.8	96	96.2

5.2 Information Extraction and Success rate prediction

As there are several attacks on the internet, botnets are considered as key vehicles and detection of botnets are challenging due to the various botnet protocols and their structures. The malware attacks on the internet are evolving rapidly and the botnet is the main factor in exploding the malwares. The performance of machine learning architectures is investigated by fine-tuning the hidden layers and neurons. The performance of botnet detection is evaluated using publicly available datasets. The experiments showed that Ensemble Classifier Algorithm with Stacking Process is better for botnet classification by achieving 94.08% accuracy, 86.5% sensitivity, 85.68% specificity, and 78.24% of F-measure. Less is taken to test and evaluate network flows' performance and identify the class as a standard or botnet attacked file [15].

5.2.1 ElasticNet Regression Model (ENetRM)

The elements measured in the physical world are integrated with manual human input, and moreover physical components are also combined with conventional social networks. In computing systems, the Cyber Physical system

(CPS) is the next stage of development with respect to the real time prediction model. When using CPS, users are able to share and store information and location gathered from devices like sensors and smart phones [16]. This enormous additional information gathered every day by the users of CPS and enterprises are more valuable for individuals as well as enterprises which helps to understand the daily activities of human, social areas, and lifestyle in a better way. With well-developed communication technologies which support Industry, the industrial cyber-physical system (ICPS) becomes a standard. In ICPS, the impacts of a thriving cyber-attack can be critical and/or broad, as ICPS are generally found in sectors like chemical, transport systems, dams and energy sectors which have critical infrastructure. The two important consequences to increase a low-and-slow attack are i) launching an attack is reduced and ii) detecting these attacks is a complex task as not classified by traffic as described in Figure 4.

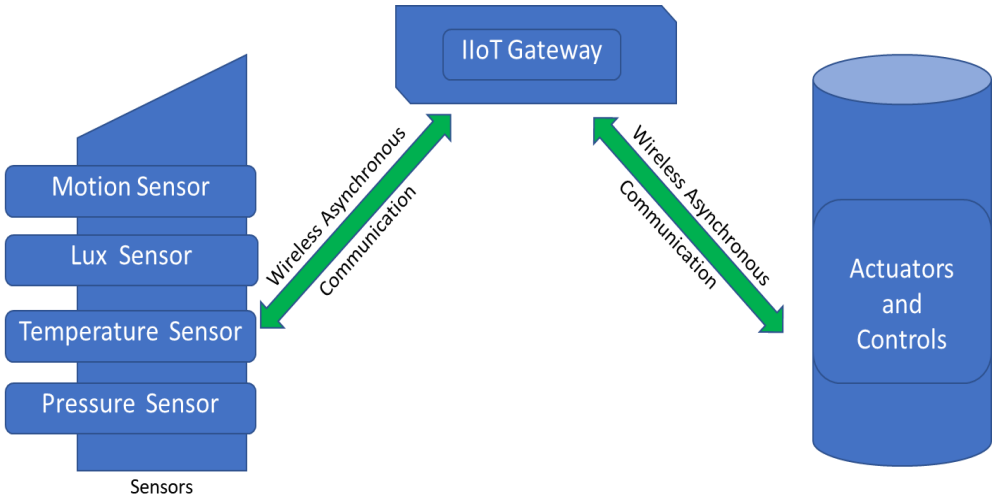

Figure 4: Three-layer architecture of ICPS system

5.2.2 ElasticNet Prediction and Deduction model

When a user is trying to access the internet, there may be access by the robot as an attacker on the server. This attacker tries to hack the group of machines at the same time. The picture in the next slide shows the system architecture for prediction of malicious traffic. It is given that a set of four servers are targeted by the robot where the data fabrication, interruption, data modification and data capturing is undergone. The internet will get two types of traffic namely malicious traffic and normal traffic. There is no problem with normal traffic but, the malicious traffic must be considered [17,18] , which can be split into training and testing phases. The

malicious data is fed as training data and by using the ElasticNet Regression Model (ENetRM), the prediction is done as a correct and falsified label as shown in Figure 5.

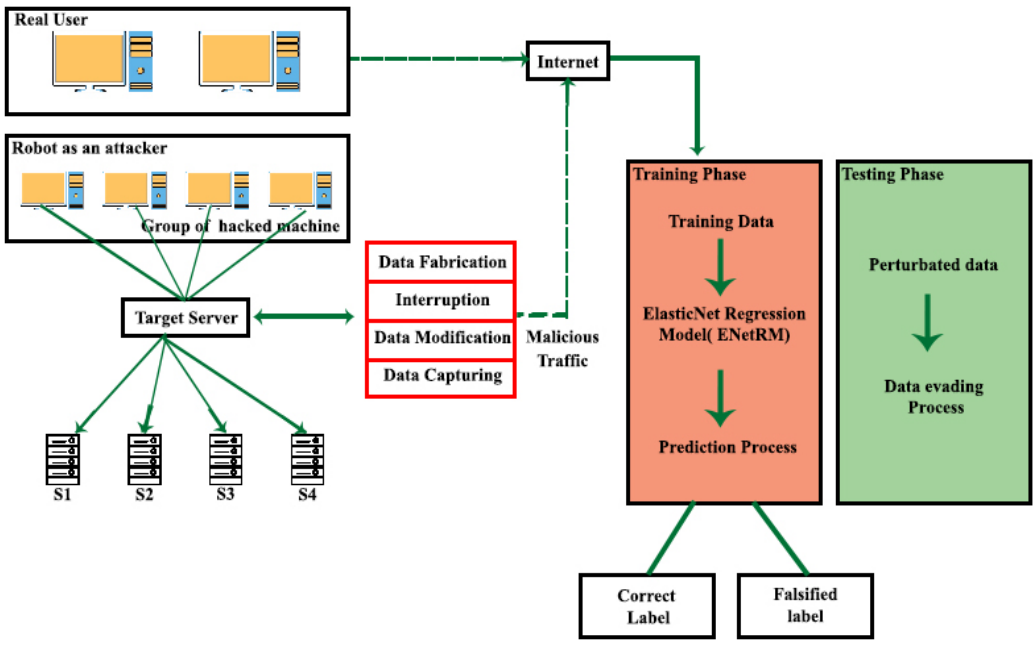

Figure 5: System architecture for prediction of malicious traffic

5.2.3 Experimental Results

During the evaluation phase, the proposed ENetRM method designed to detect cyber-attacks on a Lync server environment including a remote desktop connection, is evaluated by implementing a test bed setup. The malicious system was implemented on an Intel Next Unit of Computing (NUC) system with Ubuntu operating system. This Lync server is the primary application used for presence, desktop sharing, video and voice calls, file transfer and ad hoc conferences.

The parameters such as precision, recall, F1-score, computational overhead, data throughput are used for performance analysis. These parameters are compared with three standard approaches namely Network based Intrusion Detection System (NIDS), Novel Nested-Arc Hidden semi-Markov Model (NAHSMM) and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) with the proposed ElasticNet Regression Model (ENetRM). The dataset has the combinations of the attacked dataset and non-attacked data. Table 2 describes complete comparison between the proposed and existing methods.

Table 2: Overall comparison between existing methods and proposed methods

Parameters	DBSCAN[20]	NAHSMM [19]	NIDS [12]	ENetRM (Proposed)
Precision	0.7751	0.7855	0.9155	0.9460
Recall	0.776	0.827	0.9235	0.9764
F1-Score	0.7907	0.782	0.8811	0.9221
Throughput (%)	93.18	94.58	95.82	97.04
Computation Overhead (%)	60.4	58.38	57.18	53.48

5.2.4 ENetRM summarization

The construction of ElasticNet Regression Model (ENetRM) provides the better output when compared with the other existing methods DBSCAN, NAHSMM, NIDS due to the following factors but not limited to.

- The proposed method uses a logical regression which helps to identify the number of malicious attacks based on the differentiated traffic. However, the existing methods are using the regular regression which identifies the attacks only to the regular traffic patterns
- The proposed pattern algorithms use differential factors to identify the false positive; Hence, the number of iterations are minimal to identify the real attacks, whereas the existing methods usually provide the false positive in every 1:13 iterations (approx.)

5.3. Stacked BiLSTM and CNN+LSTM-Based Classification

A new technique employing deep neural networks for malware identification that considers CNN+LSTM networks' learning features automated out of the unprocessed information for catching the malicious file framework patterns and code sequence patterns. This considerably lessens the expense of artificial features engineering. We craft and apply BiLSTM malware classification methodology and resolve functional issues alongside parallel computation for BiLSTM and noise information processing. Also, we additionally employ a metaheuristic optimization

algorithm that is called the mayfly algorithm for feature selection to join networks' outcomes for enhancing the detection precision [20].

The outcomes show that BiLSTM and CNN+LSTM networks classification surpasses much of the other associated techniques on malware detection precision and acquires a supreme detecting proficiency. Detection of anomalies produces paradigm conducts of networks and the rest of the widgets and latterly seeks anomalous conduct patterns at an important quicker rate. The goal of employing an enhanced UNSW dataset alongside deep learning is for considering that the traditional machine learning approaches could consume a long duration, and the dimension of the dataset couldn't impact the prosecution of machine learning approaches described in Figure 6.

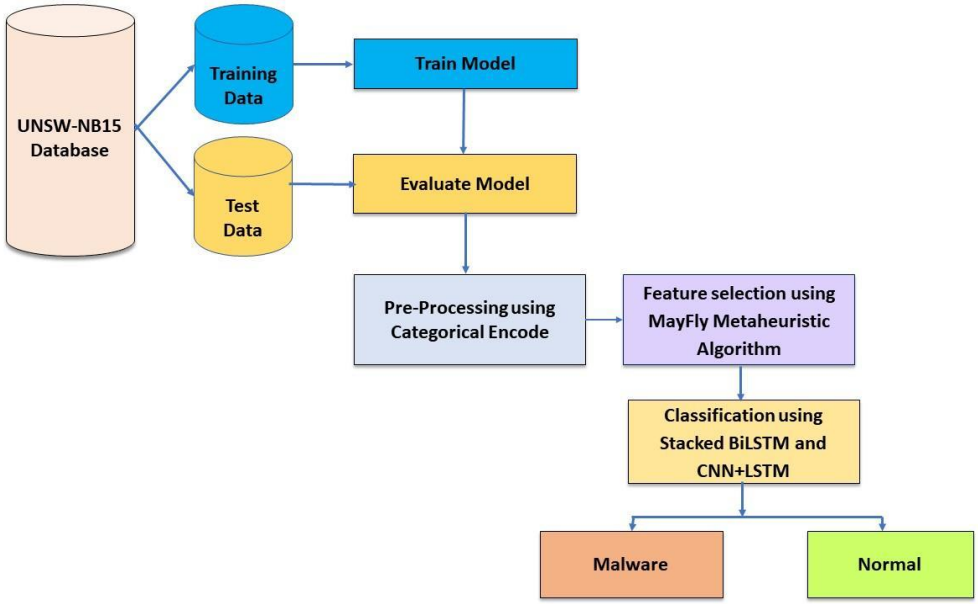

Figure 6: System architecture for malicious detection

5.3.1 Crossover betwixt mayflies and Mutation of Mayflies

The Continuous Bag of Word model (**Crossover betwixt mayflies)** is model which provides the crossover procedure. This procedure is performed by primarily choosing a male Mayfly and later a female. This choice is performed on their fitness value, that is, the finest male mates with the finest female. Two offspring are developed following a crossover as exhibited in the below equations.

$$\text{offspring1} = r_{of} * \text{male} + (1 - r_{of}) * \text{female} \quad (4)$$

$$\text{offspring2} = r_{of} * \text{female} + (1 - r_{of}) * \text{male} \quad (5)$$

In this, male denotes the parent male Mayfly, female denotes female parent, and r_{of} denotes stipulated value betwixt zero and one. Offspring's original velocity is fixed as zero.

Mutation of Mayflies: Recently produced offspring are mutated for improving exploration capacity of algorithms. Normally dispensed haphazard number is included in offspring's variable as defined in following equation.:

$$\text{offspring}_n = \text{offspring}_n + k \quad (6)$$

in which κ represents the normally distributed haphazard value

5.3.2 Convolution Neural Network and Long Short-Term Memory

This phase uses the vectors obtained from CBOW and then features are extracted using Convolution Neural Network (CNN). Further the features are optimized using Long Short-Term Memory (LSTM). LSTM retains the long-distance context information which is used for the precise classification of text. The LSTM has three gates as indicated in Figure 7. The first is the forget gate whose job is to decide which context information to be retained and which unnecessary data to be removed. Followed by the forget gate, there will be an input gate, which stores the new information. It has two layers, sigmoid layer and tanh layer. The sigmoid layer determines the information to be updated and the tanh layer creates new candidate information. In the output gate, the sigmoid layer finds the status of the output and tanh layer processes the output information.

A stacked BiLSTM as shown in Figure 8 computes the input sequence $x=(x_1, x_2,\ldots, x_n)$ out of the reverse trajectory towards the forward hidden sequence $h\rightarrow t=h\rightarrow 1,h\rightarrow 2,\ldots,h\rightarrow n$ and backward hidden sequence $h\leftarrow t=h\leftarrow 1,h\leftarrow 2,\ldots,h\leftarrow n$. Encoded vector yt is created by concatenation of last forward and backward outputs $yt=h\rightarrow t,h\leftarrow t$.

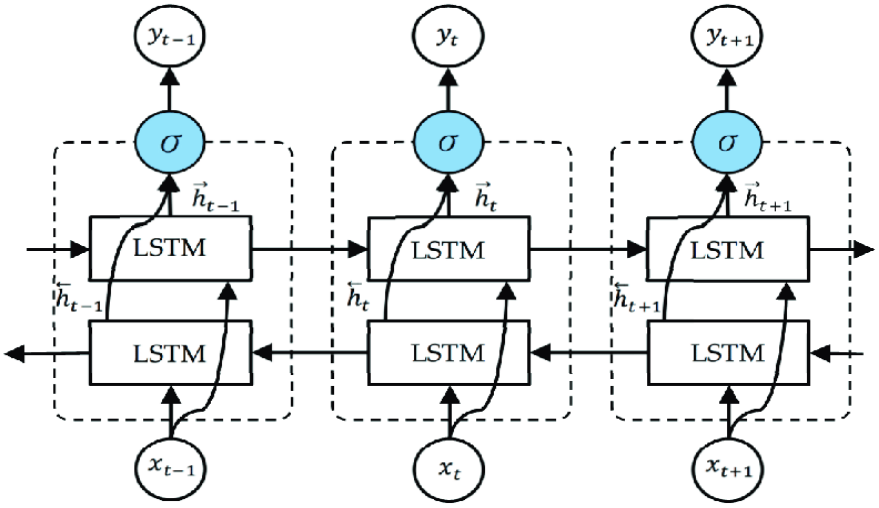

Figure 7: BiLSTM framework adopted for malware classification

$$h \rightarrow t = \sigma \quad (7)$$

$$W_h \rightarrow xxt + W_h \rightarrow h \rightarrow h \rightarrow t-1 + b_h \rightarrow h \rightarrow t = \sigma \quad (8)$$

$$W_h \rightarrow xxt + W_h \rightarrow h \rightarrow h_t + 1 + b_h \rightarrow yt = W_{yh} \rightarrow h \rightarrow t + W_{yh} \rightarrow h \rightarrow t + b \quad (9)$$

wherein $y=(y_1, y_2, \ldots y_t \ldots, y_n)$ indicates output sequence of initial hidden layer. We described a stacked BiLSTM network in which output, y_t out of the below layer turns into input of the above layer.Stacked BiLSTM architecture is exhibited in the Figure8.

$$h_t = Whh \dot{} h \rightarrow t + Whh \dot{} h \leftarrow t + b_h \quad (10)$$

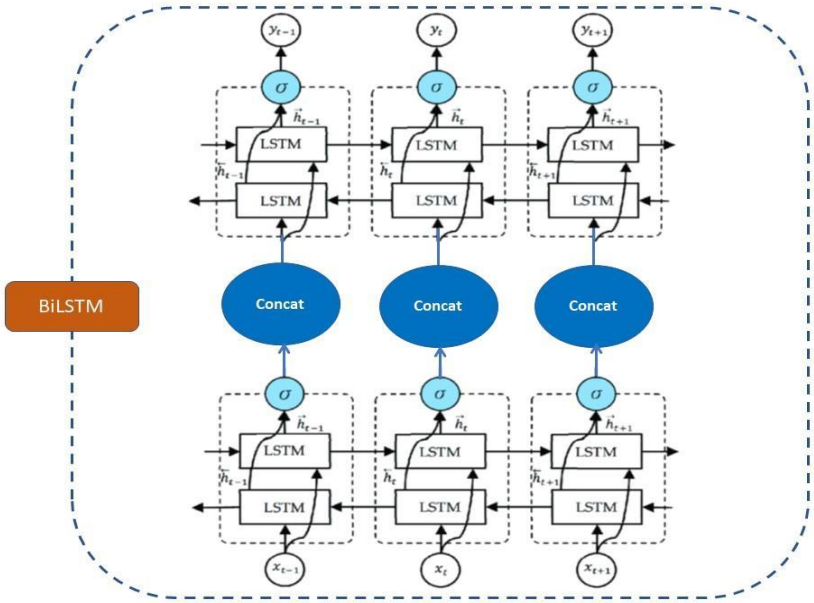

Figure 8: Stacked BiLSTM framework adopted for malware classification

Figure 9 describes the correlation of precision betwixt prevailing and proffered methods, F1-Score, accuracy score and recall.

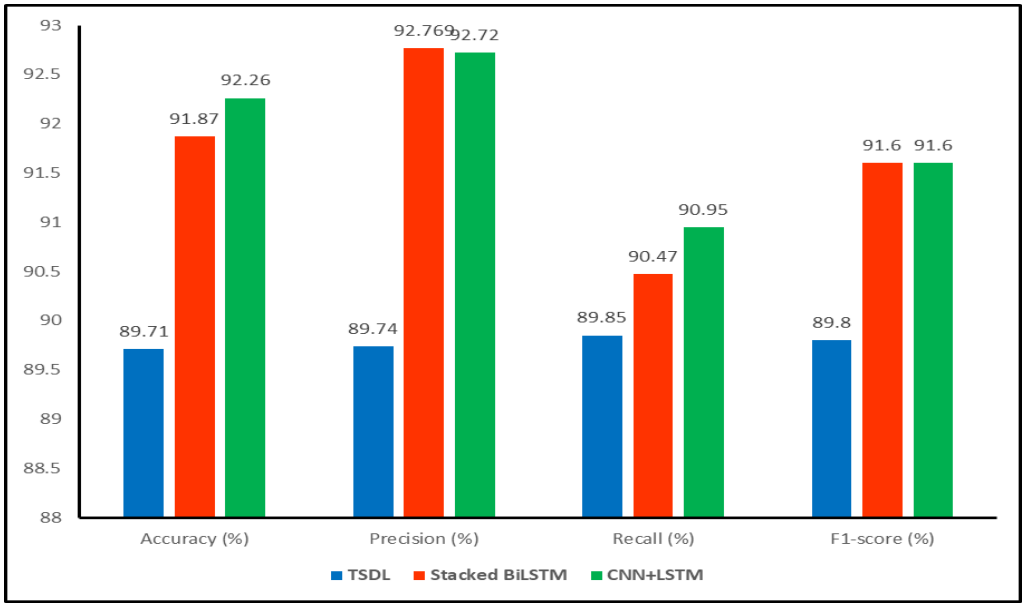

Figure 9: Correlation of precision betwixt prevailing and proffered methods, F1-Score, accuracy score and recall

Table 3 describes the existing and proposed models which are prevailing and proffered methods.

Table 3: Metrics for validating the results for the proposed and existing methods

Criteria	TSDL		Stacked BiLSTM		CNN+LSTM	
	Training	Testing	Training	Testing	Training	Testing
Accuracy (%)	89.15	90.87	89.93	91.07	90.35	92.27
Precision (%)	89.29	91.63	89.95	92.72	90.37	93.76
Recall (%)	89.15	91.03	89.32	91.93	90.12	92.97
F1-score (%)	88.87	90.9	89.47	91.6	90.53	92.69

6 ORGANIZATION OF THESIS

Chapter 1 - *"**Introduction**"* describes the basic terminologies in cyber security and malware classifications. The current concepts adapted in the malware deductions are discussed along with its advantages and disadvantages. The research

motivation and objective to overcome the mentioned drawbacks along with the contribution and organization is elaborated.

Chapter 2 - *"**Literature Review**"* elaborates the current analytical research in cyber security malware deduction proposed model and the associated existing techniques used for malware detection. In addition to, discussing various malware analysis and techniques and classification, furthermore, the advantages and disadvantages associated with existing techniques are discussed.

Chapter 3 - *"**Design and Implementation of identifying the real users from robot with unusual variation in the number of servers accessed over time using Regression base model",*** which provides the users have been authenticated and authorized from the robot users which is the optimal solutions of malware analysis and deductions

Chapter 4 - *"**Design and Implementation of users who have a high positive or negative slope to find users with unusual activity",*** provides the optimal solution of impacted users who has a fluctuated slope which finds the users unusual activity based on the malicious attack using the proposed ENetRM technique.

Chapter 5 - **"*Design and Implementation of malware analysis and techniques using Stacked BiLSTM and CNN+LSTM using Mayfly for optimization"*** provides the optimal solutions of deducting techniques and optimization Further CNN and hyper parameter tuning is explained to anticipate the outcome of the deduction. Finally, comparison analysis of the proposed approach with the existing approaches is carried out.

Chapter 6 - "***Conclusion and Future work"***, specifies the research contributions and future research perspectives.

REFERENCES

[1] P. Agrawal, & B.Trivedi, A survey on android malware and their detection techniques, Proceedings of the Third International Conference on Electrical, Computer and Communication Technologies (ICECCT), (2019).

[2] Sarah Wassermann, Pedro Casas., BIGMOMAL - Big Data Analytics for Mobile Malware Detection, Proceedings of the ACM SIGCOMM Workshop on Traffic Measurements for Cybersecurity **(**2018**).**

[3] Mohd Anul Haq, Abdul Khadar Jilani and P. Prabu, Deep Learning Based Modeling of Groundwater Storage Change, Computers, Materials & Continua, **70** (3), (2021), 4599-4617.

[4] K. S. Bhuvaneshwari1, K. Venkatachalam, S. Hubálovský, P. Trojovský, P. Prabu, Improved Dragonfly Optimizer for Intrusion Detection Using Deep Clustering CNN-PSO, Classifier, Materials & Continua, **70** (3), (2021), 5949-5965.

[5] X. Dong, C. Dong, Z. Chen, Y.Cheng, & B. Chen. BotDetector: An extreme learning machine-based Internet of Things botnet detection model, *Transactions on Emerging Telecommunications Technologies*, **32** (5) (2021).

[6] S. Bagui, E. Kalaimannan, S. Bagui, D. Nandi, & A. Pinto., Using machine learning techniques to identify rare cyber-attacks on the UNSW-NB15 dataset,. *Security and Privacy*, **2** (6) (2019)

[7] F. Peters, TT.. Tun, Y. Yu, & B. Nuseibeh. Text filtering and ranking for security bug report prediction, *IEEE Transactions on Software Engineering*, **45** (6) (2017), 615-631

[8] Ali, I., Ahmed, A. I. A., Almogren, A., Raza, M. A., Shah, S. A., Khan, A., & Gani, *A. Systematic literature review on IoT-based botnet attack., IEEE Access* (2020).

[9] A.R. Abdellah,. &A. Koucheryavy, Deep Learning with Long Short-Term Memory for IoT Traffic Prediction, Proceedings of the International Conference on Internet of Tings, Smart Spaces, and Next Generation Networks and Systems, (2020) 267–280.

[10] P. Barthakur, M. Dahal and M. K. Ghose., A Framework for P2P Botnet Detection Using SVM. Proceedings of the International Conference on *Cyber-Enabled Distributed Computing and Knowledge Discovery, (2012)* 195–200.

[11] S.K. Fayaz, Y. Tobioka, V. Sekar, and M. Bailey. *Bohatei: Flexible and elastic ddos defense*, Proceedings of the 24th USENIX Security Symposium, (2015) 817–832

[12] M. Siracusano, M., S. Shiaeles., and B. Ghita.. *Detection of IDDOS attacks based on TCP connection parameters*. Proceedings of the Global Information Infrastructure and Networking Symposium, (2008), 1–6.

[13] S. Specht, and R. Lee. *Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures*. Technical report, Princeton Architecture Laboratory for Multimedia and Security (2003).

[14] J. Saxe and K. Berlin, *Deep neural network based malware detection using two dimensional binary program features*, Proceedings of the 10th International Conference on Malicious and Unwanted Software, (MALWARE '15), (2015) 11–20.

[15] Abd Elaziz M., Shehabeldeen T. A., Elsheikh A. H., Zhou J., Ewees A. A., & Al-qaness M. A., *Utilization of Random Vector Functional Link integrated with Marine Predators Algorithm for tensile behaviour prediction of dissimilar friction stir welded aluminium alloy joints*, Journal of Materials Research and Technology, **9** (5) (2020), 11370–11381.

[16] CS. Yang, LY. Chuang, JC. Li, CH. Yang, *Chaotic maps in binary particle swarm optimization for feature selection*, Proceedings of the IEEE Conference on Soft Computing in Industrial Applications (2008) 107–112

[17] E. Emary, HM. Zawbaa, C. Grosan, AE. Hassenian, *Feature subset selection approach by Gray-Wolf optimization*, Advances in Intelligent Systems and Computing, **334** (2015).

[18] T. Kim., B. Kang, M. Rho, S. Sezer & E.G. Im., *A multimodal deep learning method for android malware detection using various features*, IEEE Transactions on Information Forensics and Security, **14** (3) 2018), 773-788.

[19] J. Feng, L. Shen, Z. Chen., Y.Wang, & H. Li., *A two-layer deep learning method for android malware detection using network traffic*, IEEE Access, **8** (2020) 125786-125796.

[20] J. Kim, J. Kim, H.L.T. Tu,, *Long short term memory recurrent neural network classifer for intrusion detection*, Proceedings of the International Conference on Platform Technology and Service, (2016).

[21] A. Chawla, B. Lee,, S. Fallon. et al. *Host based intrusion detection system with combined CNN/RNN model*, Proceedings of the Joint European Conference on Machine Learning and Knowledge Discovery in Databases, (2018) 149–158.

LIST OF PUBLICATIONS

Journal Publications

- Sathiyandrakumar Srinivasan, P Deepalakshmi, "ENetRM: ElasticNet Regression Model based malicious cyber-attacks prediction in real-time server", Measurement: Sensors, Elsevier, **25**, February 2023.

- Sathiyandrakumar Srinivasan, P Deepalakshmi, "Enhancing the security in cyber-world by detecting the botnets using ensemble classification based machine learning", Measurement: Sensors, Elsevier, **25**, February 2023.

- Sathiyandrakumar Srinivasan, P Deepalakshmi, "An innovative malware detection methodology employing the amalgamation of stacked BiLSTM and CNN+LSTM-based classification networks with the assistance of Mayfly metaheuristic optimization algorithm in cyber-attack", Concurrency And Computation: Practice And Experience. doi:10.1002/cpe.7679

- Sathiyandrakumar Srinivasan, P Deepalakshmi, " Data science in cyber security and data privacy using cyber intelligence", Cybernetics and Systems.(Under Review, IF : 2.423)

Conference Publications

- Sathiyandrakumar Srinivasan; P. Deepalakshmi, "Malware Multi Perspective Analytics with Auto Deduction in Cybersecurity", Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 11-13 November 2021. (Available in IEEE Explorer)